Saxenda® (liraglutide) injection 3 mg is an FDA-approved, prescription injectable medicine that, when used with a low-calorie meal plan and increased physical activity, may help some adults with excess weight^a who also have weight-related medical problems (such as high blood pressure, high cholesterol, or type 2 diabetes), or obesity,^b to lose weight and keep it off.
^a Body mass index (BMI) ≥27. ^b BMI ≥30.
Scroll to see Important Safety Information
Indications and Usage
What is Saxenda®?
Saxenda® (liraglutide) injection 3 mg is an injectable prescription medicine that may help some adults with excess weight (BMI ≥27) who also have weight-related
Please click here for Prescribing Information and Medication Guide.

BRENDAN I. KOERNER SECURITY 10.23.16 5:00 PM

Inside the Cyberattack That Shocked the US Government

SEÑOR SALME

SHARE

36

The US OFFICE of Personnel Management doesn't radiate much glamour. As the human resources department for the federal government, the agency oversees the legal minutiae of how federal employees are hired and promoted and manages benefits and pensions for millions of current and retired civil servants. The core of its own workforce, numbering well over 5,000, is headquartered in a hulking Washington, DC, building, the interior of which has all the charm of an East German hospital circa 1963. It's the sort of place where paper forms still get filled out in triplicate.

The routine nature of OPM's business made the revelations of April 15, 2015, as perplexing as they were disturbing. On that morning, a security engineer named Brendan Saulsbury set out to decrypt a portion of the Secure Sockets Layer (SSL) traffic that flows across the agency's digital network. Hackers have become adept at using SSL encryption to cloak their exploits, much as online vendors use it to shield credit card numbers in transit. Since the previous December, OPM's cybersecurity staff had been peeling back SSL's camouflage to get a clearer view of the data sloshing in and out of the agency's systems.

Related Stories

BRENDAN I. KOERNER
Why ISIS Is Winning the Social Media War

KIM ZETTER
The Massive OPM Hack Actually Hit 21 Million People

ANDY GREENBERG
OPM Now Admits 5.6m Feds' Fingerprints Were Stolen By Hackers

Soon after his shift started, Saulsbury noticed that his decryption efforts had exposed an odd bit of outbound traffic: a beacon-like signal pinging to a site called opmsecurity.org. But the agency owned no such domain. The OPM-related name suggested it had been created to deceive. When Saulsbury and his colleagues used a security program called Cylance V to dig a little deeper, they located the signal's source: a file called mcutil.dll, a standard component of software sold by security giant McAfee. But that didn't make sense; OPM doesn't use McAfee products. Saulsbury and the other engineers soon realized that mcutil.dll was hiding a piece of malware designed to give a hacker access to the agency's servers.

The Office of Personnel Management repels 10 million attempted digital intrusions per month—mostly the kinds of port scans and phishing attacks that plague every large-scale Internet presence—so it wasn't too abnormal to discover that something had gotten lucky and slipped through the agency's defenses. In March 2014, for example, OPM had detected a breach in which blueprints for its network's architecture were siphoned away. But in this case, the engineers noticed two unusually frightening details. First, opmsecurity.org had been registered on April 25, 2014, which meant the malware had probably been on OPM's network for almost a year. Even worse, the domain's owner was listed as "Steve Rogers"—the scrawny patriot who, according to Marvel Comics lore, used a vial of Super-Soldier Serum to transform himself into Captain America, a member of the Avengers.

> **Based on the little he'd heard about the malware, Mejeur was certain his investigation would uncover plenty of nasty surprises.**

Registering sites in Avengers-themed names is a trademark of a shadowy hacker group believed to have orchestrated some of the most devastating attacks in recent memory. Among them was the infiltration of health insurer Anthem, which resulted in the theft of personal data belonging to nearly 80 million Americans. And though diplomatic sensitivities make US officials reluctant to point fingers, a wealth of evidence ranging from IP addresses to telltale email accounts indicates that these hackers are tied to China, whose military allegedly has a 100,000-strong cyberespionage division. (In 2014 a federal grand jury in Pennsylvania indicted five people from one of that division's crews, known as Unit 61398, for stealing trade secrets from companies such as Westinghouse and US Steel; all the defendants remain at large.)

Once Captain America's name popped up, there could be little doubt that the Office of Personnel Management had been hit by an advanced persistent threat (APT)—security-speak for a well-financed, often state-sponsored team of hackers. APTs like China's Unit 61398 have no interest in run-of-the-mill criminal activities such as selling pilfered Social Security numbers on the black market; they exist solely to accumulate sensitive data that will advance their bosses' political, economic, and military objectives. "Everyone can always say, 'Oh, yeah, the Pentagon is always going to be a target, the NSA is always going to be a target,'" says Michael Daniel, the cybersecurity coordinator at the White House, who was apprised of the crisis early on. "But now you had the Office of Personnel Management as a target?"

To figure out why the hackers had trained their sights on OPM, investigators would have to determine what, if anything, had been stolen from the agency's network over the preceding year. But first they had to hunt down and eliminate the malware on its network, an archaic monstrosity that consisted of as many as 15,000 individual machines.

CURTIS MEJEUR WAS a victim of dreadful timing. A wry and diminutive former marine who had served in Fallujah, where he mapped insurgent strongholds as part of an intelligence unit dubbed the Hobbits, Mejeur started work as one of OPM's senior IT strategists on April 1, 2015. He was still getting acclimated to his new job when, on the morning of April 16, he was handed the most daunting assignment of his career: Lead the effort to snuff out the attack on the agency's network.

Based on the little he'd already heard about the malware's power and lineage, Mejeur was certain his investigation would uncover plenty of nasty surprises. But he wouldn't have to deal with them alone; early that morning, a team of engineers from the US Computer Emergency Readiness Team, the Department of Homeland Security unit that handles digital calamities, marched into OPM's headquarters. The engineers set up a command post in a windowless storage room in the subbasement, just down the hall from where Saulsbury had discovered the hack less than 24 hours earlier.

Since they couldn't trust OPM's compromised network, the visitors improvised their own by lugging in workstations and servers that they could seal behind a customized firewall. Soon enough, the subbasement was filled with the incessant clatter of keyboards, occasionally punctuated by the hiss of a Red Bull being popped open. The dozen-plus engineers rarely uttered more than a few words to one another, which is how they prefer to operate.

One of the US-CERT team's first moves was to analyze the malware that Saulsbury had found attached to mcutil.dll. The program turned out to be one they knew well: a variant of PlugX, a remote-access tool commonly deployed by Chinese-speaking hacking units. The tool has also shown up on computers used by foes of China's government, including activists in Hong Kong and Tibet. The malware's code is always slightly tweaked between attacks so firewalls can't recognize it.

The hunt to find each occurrence of PlugX continued around the clock and dragged into the weekend. A sleeping cot was squeezed into the command post, where temperatures became stifling when the building's air conditioners shut off as usual on Saturdays and Sundays.

The hunt turned up not just malware but also the first inklings of the breach's severity. A technician from the security software company Cylance, who was supporting the effort, spotted encrypted .rar files that the attackers had neglected to delete. He knew that .rar files are used to store compressed data and are often employed by hackers to shrink files for efficient exfiltration. In an email to Cylance CEO Stuart McClure on Sunday, April 19, the technician was blunt in his assessment of OPM's situation: "They are fucked btw," he wrote.

By Tuesday the 21st, having churned through a string of nearly sleepless days and nights, the investigators felt satisfied that they'd done their due diligence. Their scans had identified over 2,000 individual pieces of malware that were unrelated to the attack in question (everything from routine adware to dormant viruses). The PlugX variant they were seeking to annihilate was present on fewer than 10 OPM machines; unfortunately, some of those machines were pivotal to the entire network. "The big one was what we call the jumpbox," Mejeur says. "That's the administrative server that's used to log in to all the other servers. And it's got malware on it. That is an 'Oh feces' moment."

By controlling the jumpbox, the attackers had gained access to every nook and cranny of OPM's digital terrain. The investigators wondered whether the APT had pulled off that impressive feat with the aid of the system blueprints stolen in the breach discovered in March 2014. If that were the case, then the hackers had devoted months to laying the groundwork for this attack.

At first, the investigators left each piece of malware in place, electing only to throttle its ability to send outbound traffic; if the attackers tried to download any data, they would find themselves confined to dial-up speeds. But on April 21, Mejeur and the US-CERT team began to discuss whether it was time to boot the attackers, who would thus learn that they'd been caught. "If I miss one remote-access tool, they'll come back in through that variant, they'll reestablish access, and then they'll go dormant for six months to a year at least," says a US-CERT incident responder who participated in the OPM investigation and who agreed to speak on the condition he remain anonymous. "And then a year later, they've now put malware in a lot of different places, and you don't know what's happening because you think you already mitigated the threat."

> **OPM has a multifactor authentication scheme, but it wasn't fully implemented until January 2015—too late to prevent the PlugX attack.**

The debate continued until the evening of Friday, April 24, when an opportunity presented itself: As part of a grid modernization program in Washington, OPM's building was scheduled to have its power cut for several hours. The team decided that, even though it would mostly be just a psychological triumph, they would dump the malware just minutes before the blackout. If the attackers were monitoring the network, they wouldn't realize their access had been cut until everything finished booting up at least 12 hours later.

By the time power was restored on the 25th, the hackers no longer had the means to roam OPM's network—or at least that's what everyone hoped. The investigators could finally turn toward piecing together what the attackers had hauled away.

THERE IS A COMMON misperception that the surest way to frustrate hackers is to encrypt data. But advanced persistent threats are skilled at routing around such measures. The first item groups like these usually swipe is the master list of credentials—the usernames and passwords of everyone authorized to access the network. The group's foot soldiers will then spend weeks or months testing those credentials in search of one that offers maximum system privileges; the ideal is one that belongs to a domain administrator who can decrypt data at will. To minimize their odds of tripping any alarms, the attackers will try each credential only once; then they'll wait hours to try the next. Since these hackers are likely salaried employees, investing that much time in an attack is just part of the job.

There is a straightforward way to foil this approach: multifactor authentication, which requires anyone logging in to a network to be in physical possession of a chip-enhanced ID card that correlates with their username and password. OPM has such an authentication scheme, but it wasn't fully implemented until January 2015—too late to prevent the PlugX attack. The beacon that connected to opmsecurity.org helped the attackers keep their foothold in the network.

When hackers utilize genuine credentials, life becomes difficult for those who specialize in postattack forensics. Investigators must determine when authorized credential holders weren't using their accounts at times when the records state otherwise. And the only way to accomplish that is through face-to-face interviews: For nearly a month, Mejeur and the US-CERT engineers grilled hundreds of OPM employees in groups of six. Since human memories are so faulty, the investigators counted themselves fortunate when an employee was able to recall that they had been on vacation while their credential was in use for a particular week; the team could then analyze that account's activity during that span, confident that a hacker was responsible for it all.

> **OPM data can include everything from lie detector results to notes about whether an applicant engages in risky sexual behavior.**

As the investigators laboriously sifted through interview transcripts and network logs, they created a rough timeline of the attack. The earliest incursion they could identify had been made with an OPM credential issued to a contractor from KeyPoint Government Solutions. There was no way to know how the hackers had obtained that credential, but the investigators knew that KeyPoint had announced a breach of its own in December 2014. There was a good chance that the hackers had first targeted KeyPoint in order to harvest the single credential necessary to compromise OPM.

Once established on the agency's network, they used trial and error to find the credentials necessary to seed the jumpbox with their PlugX variant. Then, during the long Fourth of July weekend in 2014, when staffing was sure to be light, the hackers began to run a series of commands meant to prepare data for exfiltration. Bundles of records were copied, moved onto drives from which they could be snatched, and chopped up into .zip or .rar files to avoid causing suspicious traffic spikes. The records that the attackers targeted were some of the most sensitive imaginable.

The hackers had first pillaged a massive trove of background-check data. As part of its human resources mission, OPM processes over 2 million background investigations per year, involving everyone from contractors to federal judges. OPM's digital archives contain roughly 18 million copies of Standard Form 86, a 127-page questionnaire for federal security clearance that includes probing questions about an applicant's personal finances, past substance abuse, and psychiatric care. The agency also warehouses the data that is gathered on applicants for some of the government's most secretive jobs. That data can include everything from lie detector results to notes about whether an applicant engages in risky sexual behavior.

> **The agency's own assistant inspector general for audits testified about a "long history of systemic failures to properly manage its IT infrastructure."**

The hackers next delved into the complete personnel files of 4.2 million employees, past and present. Then, just weeks before OPM booted them out, they grabbed approximately 5.6 million digital images of government employee fingerprints.

When OPM went public with news of the hack in early June, speculating about the attackers' plans for the data became a popular Beltway pastime: Some of the theories involved a Chinese plot to recruit agents and, more outlandishly, a scheme to graft fingerprints onto Chinese spies so they could foil biometric sensors. But concrete evidence of the hackers' long-term intentions remains virtually nonexistent, which may be the scariest part of all.

"We haven't seen a single indication of this data being used anywhere," says Arun Vishwanath, a cybersecurity researcher at the State University of New York at Buffalo. "Yeah, we know the data is gone, but where did it go? What's the purpose of all of this? No one has the answer to any of that."

THE CONGRESSIONAL HEARINGS that take place in the wake of national calamities often have a vicious edge, and the one looking into the OPM hack was no exception. The agency's director, Katherine Archuleta, turned in a clumsy performance before the House Oversight Committee: She failed to offer a clear idea of how many people had been affected by the attack, and she seemed to duck personal responsibility by repeatedly mentioning how difficult it is to secure OPM's aging "legacy systems." The committee's members reacted with predictable scorn.

"I wish that you were as strenuous and hardworking at keeping information out of the hands of hackers as you are keeping information out of the hands of Congress and federal employees," chided representative Stephen Lynch (D-Massachusetts).

Damning details about OPM's porous security emerged at the hearing. The agency's own assistant inspector general for audits testified about what he characterized as a "long history of systemic failures to properly manage its IT infrastructure."

The tone of the hearings struck some observers as overly brutal. The OPM brain trust received no credit for implementing the SSL decryption program that had led to the attack's discovery, nor for acting fast to quell the threat. "They could easily have just buried all this stuff and no one would ever have known," says Stuart McClure, the Cylance CEO. "But they were highly pro-active—they just wanted to do what was right."

But political dramas of this sort seldom end in acts of mercy: Archuleta resigned under pressure, and her CIO, Donna Seymour, opted for retirement days before she was to endure another round of grilling by the House committee. The two executives' departures struck fear into their peers across the federal bureaucracy. "It was easy for people to see themselves in OPM and ask the question 'What do we have that people might care about that we hadn't thought about before?'" says Michael Daniel, the White House cybersecurity coordinator who previously spent over a decade overseeing the intelligence community's budget while at the Office of Management and Budget.

These newly frightened agency heads made for a receptive audience during the Cybersecurity Sprint, a White House initiative that aimed to improve security throughout the government in a mere 30 days. Held in June 2015, the Sprint was the idea of Tony Scott, who had become the third-ever US federal CIO just five months earlier. "Don't waste a good crisis," says Scott, a bearlike and avuncular veteran of Microsoft and Disney. He pressed agencies to spend the Sprint focusing on what he terms "basic hygiene"—that is, making simple upgrades that can drastically reduce an organization's susceptibility to attack. These include measures such as keeping current with the latest software patches, reducing the number of network users with administrative privileges, and, above all, broadening the adoption of multifactor authentication. According to Scott, the federal government's use of smartcards for multifactor authentication increased by more than 70 percent during the Sprint.

As the Sprint neared its end in July, Scott and Daniel began to work on a longer-term response to the OPM fiasco—a set of policy goals that they hoped would revolutionize the federal government's approach to cybersecurity. The document they eventually produced, with substantial input from the likes of the Pentagon and the National Institute of Standards and Technology, became known as the Cybersecurity National Action Plan. First publicly announced by President Obama in February 2016, it calls for billions to be set aside for several critical projects, such as upgrading outmoded systems.

> **"We can't operate with the mindset that everything is about keeping them out. We have to operate knowing that they're going to get inside sometimes."**

CNAP also stresses the need for better cooperation between the private and public sectors—something that might have made the OPM hack far less severe. In February 2015, in its published analysis of the Anthem hack, the security firm ThreatConnect wrote about its discovery of a suspicious domain registered to "Tony Stark"—the alter ego of Iron Man. That domain was named opm-learning.org. Had anyone at OPM been made aware of ThreatConnect's finding that month, the agency's security staff might have started to look for malware right away. But the tip never reached the subbasement at OPM headquarters.

But the plan pays too little attention to a fundamental flaw in our approach to security: We're overly focused on prevention at the expense of mitigation. One reason these attackers can do so much damage is that the average time between a malware infection and discovery of the attack is more than 200 days, a gap that has barely narrowed in recent years.

"We can't operate with the mindset that everything has to be about keeping them out," says Rich Barger, ThreatConnect's chief intelligence officer. "We have to operate knowing that they're going to get inside sometimes. The question is, how do we limit their effectiveness and conduct secure business operations knowing they're watching?" Accomplishing that means building networks that are designed to limit a hacker's ability to maneuver and creating better ways to detect anomalous behavior by allegedly authorized users.

A cybersecurity overhaul of this magnitude will, of course, require an abundance of talent. And that means much depends on how well government recruiters can convince the best engineers that being locked in a high-stakes competition with supervillain-esque adversaries is more exciting than working in Silicon Valley. Perhaps it will be an easy sell. After all, improving a commercial antivirus program, no matter how highly paid a gig, simply doesn't have the romantic appeal of battling Unit 61398 for world supremacy.

This article appears in our special November issue, guest-edited by President Barack Obama. Subscribe now.

#LONGREADS #MAGAZINE-24.11

VIEW COMMENTS

SPONSORED STORIES POWERED BY OUTBRAIN

LIVESTLY
[Pics] The Purpose Behind The Little Pocket On Underwear

RANKER
Here's What The Hunger Games Characters Were Supposed To...

CROWDYFAN
[Pics] Mom Kicked Off Plane Over Outfit

GADGETHEORY
[Gallery] Female Cop Hid Her Double Life For 7 Years

POSTFUN
20 Movies So Disturbing People Walked Out Of The...

SECURITY
AN AI THAT READS PRIVACY POLICIES SO THA...
ANDY GREENBERG

We Recommend
POWERED BY OUTBRAIN
SPONSORED
50 Maps Of The USA That Made Us Say 'Whoa'
RANKER

SECURITY
The WIRED Guide to Digital Security
WIRED STAFF

PODCASTS
'Palm Springs' Is 'Groundhog Day' With a Twist

PODCASTS
THIS BOOK WILL CHANGE HOW YOU SEE 'GAME OF THRONES'
GEEK'S GUIDE TO THE GALAXY

FICTION
'The Confessions': What If All Your Secrets Became Public?
JOSHUA COHEN

SECURITY
Your Handy Guide to the Many Tech Anxieties of Our Time
WIRED STAFF

GET WIRED ACCESS 1 YEAR FOR $10
SUBSCRIBE NOW

GET OUR NEWSLETTER
WIRED's biggest stories, delivered to your inbox.
Enter your email
SUBMIT

WE'RE ON PINTEREST
FOLLOW

CNMN Collection

© 2018 Condé Nast. All rights reserved.

Use of and/or registration on any portion of this site constitutes acceptance of our User Agreement (updated 5/25/18) and Privacy Policy and Cookie Statement (updated 5/25/18). Your California Privacy Rights. The material on this site may not be reproduced, distributed, transmitted, cached or otherwise used, except with the prior written permission of Condé Nast. Ad Choices.